Listing of the Claims:

1. (currently amended) A method of transmitting a signal to a receiver in order to allow the receiver to acquire synchronization to the signal, comprising:

generating a sequence of pseudorandom noise chips according to a pseudorandom noise code to produce a transmit signal;

amplifying the transmit signal during time intervals to produce higher power pulses that are separated in time, wherein time intervals between successive higher power pulses are determined based on a cryptographic sequence and represents synchronization information for said transmit signal; and

transmitting the transmit signal to the receiver to allow the receiver to use knowledge of the cryptographic sequence to acquire synchronization to the signal.

2-12. (canceled)

13. (currently amended) A transmitter suitable for transmitting a staggered pulse signal, comprising:

a code generator configured to generate a plurality of pulses according to a code to produce a transmit signal;

a cryptographic unit configured to generate a cryptographic sequence based on a cryptographic key; and

an amplifier connected to the code generator and the cryptographic unit, wherein the amplifier amplifies the transmit signal to a higher level during short bursts of time that are separated in time, wherein time intervals between successive short bursts are determined based on said cryptographic sequence and represents synchronization information for the transmit signal so as to allow a receiver that receives the transmit signal to use knowledge of the cryptographic sequence to acquire synchronization to the transmit signal.

14. (original) The transmitter of claim 13, wherein the code is a pseudorandom noise (PN) code.

15. (canceled)

16. (currently amended) A transmitter suitable for transmitting a staggered pulse signal, comprising:

code generator means for generating a plurality of pulses according to a code to produce a transmit signal;

means for generating a cryptographic sequence based on a cryptographic key; and

means for amplifying connected to said code generator means and said means for generating, wherein the means for amplifying amplifies the transmit signal to a higher level during short bursts of time that are separated in time, wherein time intervals between successive short bursts are determined based on said cryptographic sequence and represents synchronization information for said signal so as to allow a receiver that receives the transmit signal to use knowledge of the cryptographic sequence to acquire synchronization to transmit signal.

17. (original) The transmitter of claim 16, wherein the code is a pseudorandom noise (PN) code.

18. (canceled)

19. (currently amended) A receiver for receiving a staggered pulse signal having high-power pulses separated by time intervals according to a cryptographic algorithm, the receiver comprising:

a cryptographic unit configured to generate a cryptographic sequence corresponding to the cryptographic algorithm; and

a code detection unit connected to the cryptographic unit and configured to detect the high-power pulses in the received staggered pulse signal to determine time intervals between bursts of the high-power pulses, wherein the code detection unit uses the cryptographic sequence in order to decode ~~decodes~~ the time intervals between successive bursts of the high-power pulses to acquire synchronization to the staggered pulse signal.

20. (original) The receiver of claim 19, wherein the code detection unit comprises:

a correlator configured to correlate the received signal with a local code and to output a correlation signal; and

a decoder unit configured to decode the correlated signal based on the cryptographic sequence generated by the cryptographic unit.

21. (previously presented) The receiver of claim 20, wherein the decoder unit comprises a matched filter configured to detect time intervals between the high power pulses of the staggered pulse signal to acquire synchronization to the staggered pulse signal.

22. (original) The receiver of claim 21, wherein the cryptographic unit comprises a cryptographic processing unit and a cryptographic storage unit having stored therein cryptographic keys, wherein the cryptographic processing unit generates the cryptographic sequence based on a key stored in the cryptographic storage unit.

23. (previously presented) The receiver of claim 19, wherein the decoder unit uses a pseudorandom noise (PN) code to decode the staggered pulse signal.

24. (currently amended) A receiver for receiving a staggered pulse signal having high-power pulses separated by time intervals according to a cryptographic algorithm, the receiver comprising:

means for generating a cryptographic sequence corresponding to the cryptographic algorithm; and

code detection means for detecting the high-power pulses to determine time intervals between bursts of the high-power pulses, wherein the code detection means uses the cryptographic sequence in order to decode ~~decodes~~ the time intervals between successive bursts of the high-power pulses to acquire synchronization to the staggered pulse signal.

25. (original) The receiver of claim 24, wherein said code detection means comprises:

means for correlating the received signal with a local code and outputting a correlation signal; and

decoder means for decoding the correlated signal based on the generated cryptographic sequence.

26. (previously presented) The receiver of claim 25, wherein said decoder means comprises filter means for detecting time intervals between the high power pulses of the staggered pulse signal.

27. (previously presented) The receiver of claim 24, wherein the code detection means uses a pseudorandom noise (PN) code to decode the staggered pulse signal.

28. (currently amended) A method of transmitting a signal to a receiver in order to allow the receiver to acquire synchronization to the signal, comprising:

generating a sequence of pseudorandom noise chips according to a pseudorandom noise code to produce a transmit signal;

increasing a power level of the transmit signal for short bursts of time that are separated by time intervals determined based on a cryptographic sequence, and wherein the time intervals represents synchronization information for the transmit signal; and

transmitting the transmit signal to the receiver to allow the receiver to use knowledge of the cryptographic sequence to acquire synchronization to the signal.

29. (previously presented) A method for receiving a staggered pulse signal comprising short bursts of higher power, wherein the short bursts are separated by time intervals according to a cryptographic algorithm, comprising:

detecting the short bursts;

determining durations of time intervals between successive short bursts; and

acquiring synchronization to the staggered pulse signal based on said durations of said time intervals using knowledge of a cryptographic sequence used to define said time intervals in the staggered pulse signal.

30. (new) A method for communication between a transmitter and an authorized receiver, comprising:

at the transmitter:

generating a pseudorandom noise sequence;

modulating a carrier signal with the pseudorandom noise sequence to produce a modulated signal;

boosting a transmit power during finite length pulses of the modulated signal to produce a transmit signal, with each pulse encompasses a plurality of code chips and such that individual pulses having different durations and time interval spacings between them, wherein the durations and time interval spacings are controlled by a cryptographic sequence, known only to the transmitter and to authorized receivers, and represents synchronization information for the transmit signal;

transmitting the transmit signal to the receiver;

at the authorized receiver:

receiving the transmit signal and producing a received signal;

detecting the individual pulses in the received signal;

determining durations of time intervals between successive pulses; and

acquiring synchronization to the transmit signal based on the durations of the time intervals using knowledge of said cryptographic sequence used to define said time intervals at the transmitter.

31. (new) A communication system comprising a transmitter and an authorized receiver, wherein the transmitter comprises:

a code generator configured to a pseudorandom noise sequence;

a modulator that modulates a carrier signal with the pseudorandom noise sequence to produce a modulated signal;

a cryptographic unit that generates a cryptographic sequence based on a cryptographic key; and

an amplifier connected to the modulator and the cryptographic unit, wherein the amplifier amplifies the modulated signal to a higher level during short bursts of time that are separated in time, wherein time intervals between successive short bursts are determined based on said cryptographic sequence known only to the transmitter and to authorized receivers, and represents synchronization information for the transmit signal; wherein the authorized receiver comprises:

a cryptographic unit that generates a cryptographic sequence that matches the cryptographic sequence used in said transmitter; and

a correlator that is configured during an acquisition mode to match only to higher power portions of the sequence having time intervals between higher power bursts based

on said cryptographic sequence in order to acquire synchronization to said transmit signal, and said correlator ignoring lower power portions of the sequence until synchronization is acquired, and thereafter switching to a tracking mode whereby said correlator correlates to the entire pseudorandom noise sequence including lower power portions.